EXHIBIT O

Exhibit O

Claim Chart for U.S. Patent No. 11,937,172

Claim	Exemplary Infringement Analysis
1. A method of operating a smartphone in performing at least one financial transaction; the method including a two-step process in establishing and using a capability in order to perform said at least one financial transaction; the method comprising:	The Accused Products perform "a method of operating a smartphone in performing at least one financial transaction; the method including a two-step process in establishing and using a capability in order to perform said at least one financial transaction." For example, using an iPhone to conduct a financial transaction via Apple Pay satisfies the method recited in claim 1. The method includes a two-step process in establishing and using a capability in order to perform said at least one financial transaction. **Use Apple Pay for contactless payments on iPhone** With your Apple Cash, credit, and debit cards stored in the Wallet app ▢ on iPhone, you can use Apple Pay for secure, contactless payments in stores, restaurants, and more. https://support.apple.com/guide/iphone/use-apple-pay-for-contactless-payments-iphbd4cf42b4/ios Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
responsive to sensing at least one parameter by at least one sensor of the smartphone and responsive to determining that	The Accused Products use a method that involves, "responsive to sensing at least one parameter by at least one sensor of the smartphone and responsive to determining that the at least one parameter that is sensed satisfies a criterion." For example, using an iPhone to conduct a financial transaction via Apple Pay includes sensing (by an iPhone, using a sensor that is part of the iPhone) at least one parameter (e.g., physiological data associated with a living organism, namely, the human user of an iPhone) and performing actions (described below) responsive to sensing the at least one parameter. Pertinent iPhone-based sensors include a camera (for Face ID) or a physical sensor (for Touch ID), which can sense

1

Claim	Exemplary Infringement Analysis
the at least one parameter that is sensed satisfies a criterion,	physiological data of the user such as facial geometry or a fingerprint. The iPhone determines that the parameter (e.g., Face ID or Touch ID) satisfies a criterion before unlocking the device. **When you use Apple Pay in stores** When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. If your iPhone is on and detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Face ID, Touch ID, or your passcode (except in Japan if you designate a Suica card for Express Transit). With Face ID or with Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment. After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment card number. Before they approve the payment, your bank, card issuer, or payment network can verify your payment information by checking the dynamic security code to make sure that it's unique and tied to your device. https://support.apple.com/en-us/HT203027 **Face ID security** With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. Face ID uses neural networks for determining attention, matching, and antispoofing, so a user can unlock their phone with a glance, even with a mask on when using supported devices. Face ID automatically adapts to changes in appearance, and carefully safeguards the privacy and security of a user's biometric data.

Claim	Exemplary Infringement Analysis
	Touch ID security Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use. Apple devices with a Touch ID sensor can be unlocked using a fingerprint. Touch ID doesn't replace the need for a device passcode or user password, which is still required after device startup, restart, or logout (on a Mac). In some apps, Touch ID can also be used in place of a device passcode or user password—for example, to unlock password-protected notes in the Notes app, to unlock keychain-protected websites, and to unlock supported app passwords. However, a device passcode or user password is always required in some scenarios (for example, to change an existing device passcode or user password or to remove existing fingerprint enrollments or create new ones). https://support.apple.com/guide/security/face-id-and-touch-id-security-sec067eb0c9e/1/web/1 Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
performing a first step of said two-step process by enabling a mode to communicate by the smartphone information requesting an authorization to establish said capability;	The Accused Products use a method that involves "performing a first step of said two-step process by enabling a mode to communicate by the smartphone information requesting an authorization to establish said capability." For example, when a Face ID or Touch ID is recognized, the iPhone is unlocked, thereby enabling a mode (the unlocked iPhone) to communicate information requesting an authorization to establish the capability.

Claim	Exemplary Infringement Analysis
	Face ID security With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. Face ID uses neural networks for determining attention, matching, and antispoofing, so a user can unlock their phone with a glance, even with a mask on when using supported devices. Face ID automatically adapts to changes in appearance, and carefully safeguards the privacy and security of a user's biometric data. **Touch ID security** Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use. Apple devices with a Touch ID sensor can be unlocked using a fingerprint. Touch ID doesn't replace the need for a device passcode or user password, which is still required after device startup, restart, or logout (on a Mac). In some apps, Touch ID can also be used in place of a device passcode or user password—for example, to unlock password-protected notes in the Notes app, to unlock keychain-protected websites, and to unlock supported app passwords. However, a device passcode or user password is always required in some scenarios (for example, to change an existing device passcode or user password or to remove existing fingerprint enrollments or create new ones). https://support.apple.com/guide/security/face-id-and-touch-id-security-sec067eb0c9e/1/web/1 Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
while the mode is enabled, and as a precursor to performing a second step of	The Accused Products use a method that involves, "while the mode is enabled, and as a precursor to performing a second step of said two-step process, transmitting by the smartphone first data to a first device requesting the authorization to establish said capability to perform said at least one financial transaction."

Claim	Exemplary Infringement Analysis
said two-step process, transmitting by the smartphone first data to a first device requesting the authorization to establish said capability to perform said at least one financial transaction; and	For example, while the iPhone is unlocked (i.e., the mode is enabled), and as a precursor to performing a financial transaction using Apple Pay, a user may transmit (by the iPhone) data to a first device (a base station) requesting authorization to establish the capability to perform a financial transaction. This occurs when the iPhone user transmits information to set up a payment method in Apple Pay by, for example, adding a credit card. To add a credit card, the iPhone transmits to the card issuer data requesting authorization to use the credit card in future financial transactions. **Add a debit or credit card** 1. Open the Wallet app ▣ on your iPhone. 2. Tap ➕. You may be asked to sign in with your Apple ID. 3. Do one of the following: • *Add a new card:* Tap Debit or Credit Card, tap Continue, then position your card so that it appears in the camera frame, or enter the card details manually. • *Apply for Apple Card:* See Set up and use Apple Card on iPhone. • *Add your previous cards:* Tap Previous Cards, then choose any cards you previously used. These cards may include the card associated with your Apple ID, cards you use with Apple Pay on your other devices, cards you added to Safari AutoFill, or cards you removed from Wallet. Tap Continue, authenticate with Face ID or Touch ID, then follow the onscreen instructions. • *Add a card from a supported app:* Tap the app of your bank or card issuer (below From Apps on Your iPhone). The card issuer determines whether your card is eligible for Apple Pay, and may ask you for additional information to complete the verification process. https://support.apple.com/guide/iphone/set-up-apple-pay-iph9b7f53382/ios

Claim	Exemplary Infringement Analysis
	When a Payment Card is added to Apple Pay When you add a new payment card (*i.e. a credit or a debit card*) to Apple Pay, here are the steps that happen behind the scenes. 1. The payment card's *PAN (Primary Account Number)*, along with other card related personal details i.e. *Your Name, Card Expiration Date*, is sent by the **Apple Wallet App** to the **Apple Pay servers**. 2. From your PAN, the Apple Pay server identifies the credit card **Issuer Bank**, and then pass the PAN and your personal details to the **Issuer Bank** requesting a *Payment Token* from the **Issuer Bank**. *Note that the Issuer Bank must have partnered with Apple Pay, and be part of the Apple Pay network in order for Apple to add that payment card onto the iPhone. If the Issuer Bank has not partnered with Apple Pay, you cannot add that card to Apple Pay.* https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7 ## Apple Pay participating banks in Canada, Latin America, and the United States Apple Pay works with many of the major credit and debit cards from the top banks. Just add your supported cards and continue to get all the rewards, benefits, and security of your cards. https://support.apple.com/en-us/HT204916

Claim	Exemplary Infringement Analysis
	Why am I being asked to verify my HRCU card? ▬ For security reasons we may need you to provide additional verification to add your HRCU card to Apple Pay. If necessary, Apple Wallet or the Apple Watch app will tell you how to verify you card. If your information is verified, you should receive an Apple Wallet or Apple Watch app notification that your card is ready for Apple Pay. If you haven'â€™t received a notification after an hour, please call us at 603.509-1297. https://www.hrcu.org/resources/faq/?faq_cat=apple-pay Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
receiving by the smartphone second data from the first device, comprising the authorization, responsive to said transmitting by the smartphone the first data; then	The Accused Products use a method that involves "receiving by the smartphone second data from the first device, comprising the authorization, responsive to said transmitting by the smartphone the first data." For example, in response to transmitting the data requesting authorization to establish the capability to perform a financial transaction, the iPhone receives from the base station the authorization (second data) from the card issuer authorizing the credit card.

Claim	Exemplary Infringement Analysis
	## Add a debit or credit card 1. Open the Wallet app ▣ on your iPhone. 2. Tap ⊕. You may be asked to sign in with your Apple ID. 3. Do one of the following: - *Add a new card:* Tap Debit or Credit Card, tap Continue, then position your card so that it appears in the camera frame, or enter the card details manually. - *Apply for Apple Card:* See Set up and use Apple Card on iPhone. - *Add your previous cards:* Tap Previous Cards, then choose any cards you previously used. These cards may include the card associated with your Apple ID, cards you use with Apple Pay on your other devices, cards you added to Safari AutoFill, or cards you removed from Wallet. Tap Continue, authenticate with Face ID or Touch ID, then follow the onscreen instructions. - *Add a card from a supported app:* Tap the app of your bank or card issuer (below From Apps on Your iPhone). The card issuer determines whether your card is eligible for Apple Pay, and may ask you for additional information to complete the verification process. https://support.apple.com/guide/iphone/set-up-apple-pay-iph9b7f53382/ios

Claim	Exemplary Infringement Analysis
	5. The **Issuer Bank** receives the *Payment Token* and *Payment-Token-Key* from the **Token Service Provider (TSP)**, and adds a *CVV-Key (i.e. public key)* to the mix. 6. The **Issuer Bank** then returns the *Payment Token*, *Payment-Token-Key* and the *CVV-Key* back to the **Apple Pay Servers**. 7. Apple Pay, uses its own **Trusted Service Manager (TSM)** and provisions the *Payment Token*, *Payment Token-Key* and *CVV-Key* and maybe other data onto the "Secure Element" i.e. the secure hardware chip on the physical iPhone device. https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7 Why am I being asked to verify my HRCU card? ━ For security reasons we may need you to provide additional verification to add your HRCU card to Apple Pay. If necessary, Apple Wallet or the Apple Watch app will tell you how to verify you card. If your information is verified, you should receive an Apple Wallet or Apple Watch app notification that your card is ready for Apple Pay. If you haven't received a notification after an hour, please call us at 603.509-1297. https://www.hrcu.org/resources/faq/?faq_cat=apple-pay Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
performing the second step of said two-step process	The Accused Products use a method that involves "performing the second step of said two-step process comprising performing a first transaction of said at least one financial transaction, responsive to detecting by the smartphone that a proximity condition is satisfied and responsive to sensing the at least one parameter and determining that the at least one parameter sensed satisfies the criterion."

Claim	Exemplary Infringement Analysis
comprising performing a first transaction of said at least one financial transaction, responsive to detecting by the smartphone that a proximity condition is satisfied and responsive to sensing the at least one parameter and determining that the at least one parameter sensed satisfies the criterion;	For example, using an iPhone to conduct a first financial transaction via Apple Pay includes performing the transaction in response to the iPhone detecting that a proximity condition is satisfied (between the iPhone and a point-of-sale terminal) and in response to sensing the parameter (e.g., physiological data) and determining that the sensed parameter satisfies the criterion. Conducting a financial transaction via Apple Pay includes recognizing and accepting a fingerprint or facial geometry associated with the user. **When you use Apple Pay in stores** When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. If your iPhone is on and detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Face ID, Touch ID, or your passcode (except in Japan if you designate a Suica card for Express Transit). With Face ID or with Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment. After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment card number. Before they approve the payment, your bank, card issuer, or payment network can verify your payment information by checking the dynamic security code to make sure that it's unique and tied to your device. https://support.apple.com/en-us/HT203027 **Face ID security** With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. Face ID uses neural networks for determining attention, matching, and antispoofing, so a user can unlock their phone with a glance, even with a mask on when using supported devices. Face ID automatically adapts to changes in appearance, and carefully safeguards the privacy and security of a user's biometric data.

Claim	Exemplary Infringement Analysis
	## Touch ID security Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use. Apple devices with a Touch ID sensor can be unlocked using a fingerprint. Touch ID doesn't replace the need for a device passcode or user password, which is still required after device startup, restart, or logout (on a Mac). In some apps, Touch ID can also be used in place of a device passcode or user password—for example, to unlock password-protected notes in the Notes app, to unlock keychain-protected websites, and to unlock supported app passwords. However, a device passcode or user password is always required in some scenarios (for example, to change an existing device passcode or user password or to remove existing fingerprint enrollments or create new ones). https://support.apple.com/guide/security/face-id-and-touch-id-security-sec067eb0c9e/1/web/1 ## Pay with your default card on an iPhone with Face ID 1. Double-click the side button. 2. When your default card appears, glance at iPhone to authenticate with Face ID, or enter your passcode. 3. Hold the top of your iPhone near the card reader until you see Done or a checkmark on the screen. ## Pay with your default card on an iPhone with Touch ID 1. Rest your finger on Touch ID. 2. Hold the top of your iPhone near the card reader until you see Done or a checkmark on the screen. https://support.apple.com/guide/iphone/use-apple-pay-for-contactless-payments-iphbd4cf42b4/ios

11

Claim	Exemplary Infringement Analysis
	Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
wherein said performing the second step of said two-step process comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that a value of the at least one parameter that is sensed satisfies	The Accused Products perform the method above, "wherein said performing the second step of said two-step process comprises sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter, by detecting a short-range signal that is transmitted by the access point, determining that a value of the at least one parameter that is sensed satisfies the criterion." For example, using an iPhone to conduct a financial transaction via Apple Pay includes sensing that the proximity condition is satisfied relative to an access point maintained by a vendor at a point of purchase counter (the point-of-sale terminal, which includes an access point). The transaction includes detecting a short-range signal that is transmitted by the access point (detecting an NFC signal from the point-of-sale device) and determining that a value of the parameter (e.g., physiological data) satisfies the criterion. Conducting a transaction via Apple Pay includes recognizing and accepting a fingerprint or facial geometry associated with the user. **When you use Apple Pay in stores** When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. If your iPhone is on and detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Face ID, Touch ID, or your passcode (except in Japan if you designate a Suica card for Express Transit). With Face ID or with Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment. After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment card number. Before they approve the payment, your bank, card issuer, or payment network can verify your payment information by checking the dynamic security code to make sure that it's unique and tied to your device. https://support.apple.com/en-us/HT203027

Claim	Exemplary Infringement Analysis
the criterion and then,	**Face ID security** With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. Face ID uses neural networks for determining attention, matching, and antispoofing, so a user can unlock their phone with a glance, even with a mask on when using supported devices. Face ID automatically adapts to changes in appearance, and carefully safeguards the privacy and security of a user's biometric data. **Touch ID security** Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use. Apple devices with a Touch ID sensor can be unlocked using a fingerprint. Touch ID doesn't replace the need for a device passcode or user password, which is still required after device startup, restart, or logout (on a Mac). In some apps, Touch ID can also be used in place of a device passcode or user password—for example, to unlock password-protected notes in the Notes app, to unlock keychain-protected websites, and to unlock supported app passwords. However, a device passcode or user password is always required in some scenarios (for example, to change an existing device passcode or user password or to remove existing fingerprint enrollments or create new ones). https://support.apple.com/guide/security/face-id-and-touch-id-security-sec067eb0c9e/1/web/1

13

Claim	Exemplary Infringement Analysis
	Pay with your default card on an iPhone with Face ID 1. Double-click the side button. 2. When your default card appears, glance at iPhone to authenticate with Face ID, or enter your passcode. 3. Hold the top of your iPhone near the card reader until you see Done or a checkmark on the screen. **Pay with your default card on an iPhone with Touch ID** 1. Rest your finger on Touch ID. 2. Hold the top of your iPhone near the card reader until you see Done or a checkmark on the screen. https://support.apple.com/guide/iphone/use-apple-pay-for-contactless-payments-iphbd4cf42b4/ios Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the at least one	The Accused Products use a method that involves, "responsive to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the at least one parameter sensed satisfies the criterion, paying for a product by selectively sending information to at least one device." For example, when conducting financial transactions via Apple Pay in response to having sensed that the proximity condition is satisfied relative to the access point and having determined that the value of the sensed parameter satisfies the criterion (as described above), an iPhone can use Apple Pay to pay for a product by selectively sending information to a device (such as the point-of-sale terminal, which is a device).

14

Claim	Exemplary Infringement Analysis
parameter sensed satisfies the criterion, paying for a product by selectively sending information to at least one device;	**Paying with cards using Apple Pay** Apple Pay can be used to pay for purchases in stores, within apps, and at websites. **Paying with cards in stores** If iPhone or Apple Watch is on and detects an NFC field, it presents the user with the requested card (if automatic selection is turned on for that card) or the default card, which is managed in Settings. The user can also go to Apple Wallet and choose a card, or when the device is locked, can: • Double-click the side button on devices with Face ID • Double-click the Home button on devices with Touch ID • Using Accessibility features that allow Apple Pay from the Lock Screen Next, before information is transmitted, the user must authenticate using Face ID, Touch ID, or their passcode. When Apple Watch is unlocked, double-clicking the side button activates the default card for payment. No payment information is sent without user authentication. After the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment. Neither Apple nor a user's device sends the full credit or debit card numbers to merchants. Apple may receive anonymous transaction information such as the approximate time and location of the transaction, which helps improve Apple Pay and other Apple products and services. https://support.apple.com/guide/security/paying-with-cards-using-apple-pay-secfbd5c0e54/1/web/1

Claim	Exemplary Infringement Analysis
	When you Pay using Apple Pay with your iPhone Apple Pay uses *NFC* to send payment data to the contactless POS terminal when you Tap & Pay . Apple Pay uses the *EMVCo's contactless suite of specifications* to pass the data from your iPhone to the contactless reader terminal. 1. When you pay using the iPhone with Apple Pay, you authenticate yourself to the iPhone device Secure Element (SE) using your biometric (i.e. fingerprint, face id or PIN). *The authentication process only authenticates you to the Secure Element (SE), and allows Apple Pay to access the information stored on the Secure Element (SE). Other than this initial Authentication process, neither the Secure Element (SE) nor the biometrics (i.e. Touch ID etc), are involved in the rest of the Apple Pay process.* https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7 3. The **POS** sends this request to the **Acquirer Bank (Merchant Bank)**, which in turn forwards it to the **Payment Network** *eg. Visa, Mastercard etc.* https://codeburst.io/how-does-apple-pay-actually-work-f52f7d9348b7

Claim	Exemplary Infringement Analysis
	Pay with your default card on an iPhone with Face ID 1. Double-click the side button. 2. When your default card appears, glance at iPhone to authenticate with Face ID, or enter your passcode. 3. Hold the top of your iPhone near the card reader until you see Done or a checkmark on the screen. **Pay with your default card on an iPhone with Touch ID** 1. Rest your finger on Touch ID. 2. Hold the top of your iPhone near the card reader until you see Done or a checkmark on the screen. https://support.apple.com/guide/iphone/use-apple-pay-for-contactless-payments-iphbd4cf42b4/ios Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
wherein said paying for a product by selectively sending information to at least one device comprises selectively and wirelessly	The Accused Products perform the method above, "wherein said paying for a product by selectively sending information to at least one device comprises selectively and wirelessly transmitting information to the at least one device using unlicensed frequencies." For example, the step of paying for a product (as described above) includes selectively transmitting information to the device (point-of-sale terminal) using an unlicensed frequency. In particular, the wireless short-range communications link used by NFC is based upon the unlicensed 13.56 MHz frequency.

Claim	Exemplary Infringement Analysis	
transmitting information to the at least one device using unlicensed frequencies; and	**Paying with cards using Apple Pay** Apple Pay can be used to pay for purchases in stores, within apps, and at websites. **Paying with cards in stores** If iPhone or Apple Watch is on and detects an NFC field, it presents the user with the requested card (if automatic selection is turned on for that card) or the default card, which is managed in Settings. The user can also go to Apple Wallet and choose a card, or when the device is locked, can: • Double-click the side button on devices with Face ID • Double-click the Home button on devices with Touch ID • Using Accessibility features that allow Apple Pay from the Lock Screen Next, before information is transmitted, the user must authenticate using Face ID, Touch ID, or their passcode. When Apple Watch is unlocked, double-clicking the side button activates the default card for payment. No payment information is sent without user authentication. After the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment. Neither Apple nor a user's device sends the full credit or debit card numbers to merchants. Apple may receive anonymous transaction information such as the approximate time and location of the transaction, which helps improve Apple Pay and other Apple products and services. https://support.apple.com/guide/security/paying-with-cards-using-apple-pay-secfbd5c0e54/1/web/1	

Claim	Exemplary Infringement Analysis
	How Does Near-Field Communication Work? Near-field communication is a wireless connectivity technology that is based on RFID. It uses induction coupling to enable communication between two compatible devices that are close. It enables users to automatically transfer data bi-directionally between two NFC-enabled devices by just touching both of them or by bringing them close to each other. NFC operates at the globally unlicensed 13.56 MHz frequency. It has three different data transfer rates – i.e., 212 kbit/s, 106 kbit/s, and 424 kbit/s. https://www.spiceworks.com/tech/networking/articles/what-is-near-field-communication/ Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.
wherein said at least one parameter comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a	The Accused Products perform the method above, "wherein said at least one parameter comprises a signal, a number, a word, a code, a velocity, an acceleration, a time-of-day, a humidity, a temperature, a height, a level of brightness, a level of darkness, a blood pressure, a heart rate, a blood content, a physiological state and/or a psychological state." For example, the parameter sensed by the iPhone is, for example, a physiological state. Pertinent iPhone-based sensors include a camera (for Face ID) or a physical sensor (for Touch ID), which can sense the physiological state of the user such as facial geometry or a fingerprint.

Claim	Exemplary Infringement Analysis
heart rate, a blood content, a physiological state and/or a psychological state.	**When you use Apple Pay in stores** When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. If your iPhone is on and detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Face ID, Touch ID, or your passcode (except in Japan if you designate a Suica card for Express Transit). With Face ID or with Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment. After you authenticate your transaction, the Secure Element provides your Device Account Number and a transaction-specific dynamic security code to the store's point of sale terminal along with additional information needed to complete the transaction. Again, neither Apple nor your device sends your actual payment card number. Before they approve the payment, your bank, card issuer, or payment network can verify your payment information by checking the dynamic security code to make sure that it's unique and tied to your device. https://support.apple.com/en-us/HT203027 **Face ID security** With a simple glance, Face ID securely unlocks supported Apple devices. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of a user's face. Face ID uses neural networks for determining attention, matching, and antispoofing, so a user can unlock their phone with a glance, even with a mask on when using supported devices. Face ID automatically adapts to changes in appearance, and carefully safeguards the privacy and security of a user's biometric data.

Claim	Exemplary Infringement Analysis
	Touch ID security Touch ID is the fingerprint sensing system that makes secure access to supported Apple devices faster and easier. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time, with the sensor continuing to expand the fingerprint map as additional overlapping nodes are identified with each use. Apple devices with a Touch ID sensor can be unlocked using a fingerprint. Touch ID doesn't replace the need for a device passcode or user password, which is still required after device startup, restart, or logout (on a Mac). In some apps, Touch ID can also be used in place of a device passcode or user password—for example, to unlock password-protected notes in the Notes app, to unlock keychain-protected websites, and to unlock supported app passwords. However, a device passcode or user password is always required in some scenarios (for example, to change an existing device passcode or user password or to remove existing fingerprint enrollments or create new ones). https://support.apple.com/guide/security/face-id-and-touch-id-security-sec067eb0c9e/1/web/1 Investigation of both the patent and the Accused Products (and other potentially infringing products) is ongoing. This chart is based on evidence and analysis reasonably accessible at this time. Telcom reserves the right to update and amend the above as the litigation progresses, including in view of discovery provided by the Defendant.